Virginia Information Technologies Agency

Security Audit Action Plan 2005

DRAFT PENDING FAC & ITIB COMMENTS

September 2005

[In response to the Auditor of Public Accounts Security Audit Report, dated July 15, 2005 issued September, 2005]

Plan to be presented to the ITIB Finance & Audit Committee in October 2005.

APA Rec	Short Title	Summary	Due Date	Responsible Person(s)	Status	Task/Comments
1.A	Develop Policies, Procedures and Standards for Infrastructure	Document policies, procedures, and standards for routers and firewalls at the data center.	01/31/2006 03/31/2006	Deason Carter		1.A.1 - Baseline security configuration standards documents for routers and firewalls are being developed and submitted to Customer Services for implementation. 1.A.2 – VITA data center policies and procedures are being updated and developed to address staffing requirements, monitoring and logging procedures, and access procedures, among others.
1.B	Develop Policies, Procedures and Standards for Infrastructure	Document and implement policies, procedures, and standards for common infrastructure elements and approve any exceptions in writing.	01/31/2006 04/30/2006	Deason Saneda		1.B.1 – Security will complete the development of security policies and standards for infrastructure operations, including policies and procedures for obtaining approval of exceptions. 1.B.2 – Customer Services will begin implementation of security policies, procedures, and standards. Due to a myriad of variables, an end date to complete the initial implementation will be determined in FY2006.

APA Rec	Short Title	Summary	Due Date	Responsible Person(s)	Status	Task/Comments
2.A	Update MOA's and Maintain Documentation for Exceptions to Server Policies	Update all sever farm Customer Service Plans to reflect current security responsibilities and policies, procedures, and standards.	01/06/2006	Carter		Customer Services is including security roles and responsibilities in the Service Plans for customer agencies. The MOA will be an attachment to the Service Agreements for the Department of Taxation, the Department of Social Services, and the Virginia Employment Commission. These are the three customer Agencies that have an MOA with VITA to operate servers in the Richmond Plaza Building (RPB) server farm.
2.B	Update MOA's and Maintain Documentation for Exceptions to Server Policies	Fully document the requests and approval of exceptions to agreed-upon policies, procedures and standards.	01/06/2006 04/30/2006	Deason Carter		2.B.1 - Security Services, in consultation with Customer Services, will develop a written procedure for documenting, approving and retaining requests for exceptions to security policies, procedures and standards. 2.B.2 - Customer Services will initially implement these for the three customer Agencies for which VITA has MOAs to operate servers in the Richmond Plaza Building (RPB) server farm.
3.	Improve Policies and Procedures over Change Management	Modify existing VITA Central change management polices and procedures to include a documented & approved rollback plan, procedures for testing changes, and procedures for the review of completed high risk changes.	12/31/2005 12/31/2005 12/31/2005 03/31/2006 03/31/2006	Carter Carter Carter Carter Carter		Modify existing policies and procedures to: (3.A.) include requirements for approved rollback (back-out) plans to support the application code changes to be implemented to enforce mandatory rollback (back-out) plans. (3.B.) require all requestors to close out change requests via appropriate Complete or In-Complete designations, along with application code changes to be implemented to enforce it. (3.C.) require that changes are approved only by those authorized, along with application code changes to be implemented to support them. (3.D.) define the requirements of which changes have to be tested prior to the change being implemented. (3.E.) include the definition of "High Risk" changes and the necessary process for appropriate reviews of completed "High Risk" changes.

APA Rec	Short Title	Summary	Due Date	Responsible Person(s)	Status	Task/Comments
4.	Update Business Impact Analysis, Risk Assessment and Disaster Recovery Plan	Update risk assessment, business impact analysis and disaster recovery plan to include executive infrastructure as quickly as possible.	11/15/05 11/15/05 12/1/05 7/31/06 12/31/06 1/15/07	Deason Deason Saneda Deason/Saneda Deason Deason		4.A. Expand the VITA Disaster Recovery (DR) plan to include operations at Customer Agency locations by: 4.A.1. Obtaining COOP/DR Plans from Customer Agencies. 4.A.2. Developing a DR Assessment template. 4.A.3. Beginning an assessment of Customer Agencies DR Plans using the DR Assessment template. 4.A.4. Revising VITA DR Plan to include operations at Customer agency locations. 4.B Complete Customer Agency security assessments. 4.C Using the security assessment results and customer agency input, begin updating the VITA BIA, RA & DR.